3GPP TSG SA WG3 Security — S3#20 **S3-010470**

16 - 19 October, 2001

Sydney, Australia

Source: **Siemens, Ericsson**

Title: **IMS access domain security and NDS**

Document for: **Discussion / Decision**

Agenda Item:

Abstract

At SA3 #19, it has been proposed to use network domain security means to secure SIP signaling between the UE and the P-CSCF. The subsequent discussion, together with liaisons sent to SA2, CN1 and CN4, seem to have created some confusion about the requirements and security measures that apply. This contribution is aimed to clarify the current discussion related to the protection of IMS signaling between UE and P-CSCF, and proposes NOT to use Rel5 network domain security means to secure this specific signaling, since end-to-end protection between UE and P-CSCF will already be provided by the IMS itself.

Overview

IMS signaling in the Rel5 core network will be secured by core network security mechanisms, i.e. IPsec ESP. The core network for the IMS extends from P-CSCF entities towards other CSCF entities, with signaling secured especially between different operators through security gateways (SEG).

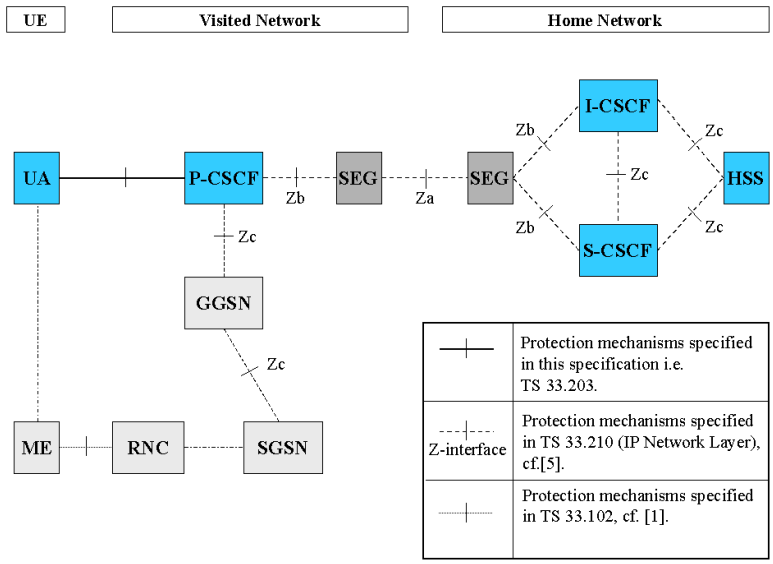

Figure 1: Relation of IMS and network domain security (as given in TS 33.203, v0.5.0)

The part of IMS signaling outside the core network is referred to as IMS access network signaling, and is the signaling taking place between UE and P-CSCF. Currently SA3 is developing a solution that protects IMS access network signaling end-to-end between the UE and the P-CSCF. The mechanism to provide IMS access network security is still open, but the working assumption is to mandate integrity protection and to optionally encrypt the signaling messages.

At SA3#19, Telenor discussed in [S3-010389] several alternatives to extend the current SA3 network domain security model to provide protection for IMS signaling between GSN entities, passing through GTP-U.

As a result of this contribution, a liaison was sent to SA2, CN1 and CN4 [S3-010403]. It listed five different options to secure IMS signaling through GTP-U:

1. To not encrypt any GTP-U messages, understanding that this means that IMS SIP messages will not be encrypted when carried by GTP-U in the core network.
2. To protect all GTP-U messages, including the small proportion that are IMS SIP messages.
3. To introduce a new sub-version of GTP for the IMS control plane (GTP-IC). This new GTP-IC would then have a unique port number assigned to it, enabling those messages to be encrypted. All IMS control plane messages would then have to be tunnelled through GTP-IC in the core network.
4. Extend GTP-C to contain all IMS control plane messages. All IMS control plane messages would then have to be tunnelled through GTP-C in the core network. Again, since GTP-C is always encrypted, the IMS SIP messages would be encrypted.
5. Introduce multiple IP addresses (multi-homing) of the CSCFs such that GTP-U containing IMS control plane messages would use a different set of IP addresses from the GTP-U containing non-IMS control plane messages.

[S3-010403] already recommended not to consider option 5 seriously.

The liaison has been responded to by [S3-010433] from SA2 and [S3-010442] from CN1.

Discussion

Reflecting the current state of discussion and the responses to [S3-010403], it seems that some confusion has been created in SA2, CN1 and even SA3, about the different possibilities to protect IMS signaling through GTP-U, and especially related to the terms "access domain" and "network domain" for the IMS and PS domain.

Used in the context of the IMS the "access network" comprises all the entities between the UE and the P-CSCF. In case GPRS is used for access, the IMS "access network" comprises all GPRS entities, i.e. SGSN and GGSN. This becomes clear from the use of the term "access network independence". In contrast, in the context of network domain security for the PS domain, SGSN and GGSN are clearly part of the core network, and not the access network, which becomes clear from the fact that the protection of GTP-C agreed by SA3 is part of NDS-IP.

Therefore, while discussing security of IMS signaling between the UE and P-CSCF, we are clearly talking about IMS access network security, and not about IMS core network security.

Actually this does not seem to have been the assumption in [S3-010389] which uses the following statement: " It is currently assumed that Network Domain Security for IP (NDS/IP) as specified in draft TS 33.210 shall also be used for protection of SIP messages in IMS." The same holds for liaison [S3-010403].

In our opinion the assumption cited above is only true for IMS core network signaling, and does not hold for IMS access network signaling.

Independent of this, it is obvious that protection for the IMS access domain signaling must be provided. The current working assumption in SA3 is at least to mandate integrity protection. Mechanisms for integrity protection and encryption are under development, to provide protection in an end-to-end fashion between the UE and the P-CSCF.

Another option could be to secure IMS access domain signalling in a hop-by-hop fashion, between the hops of the underlying PS domain. This would mean to provide protection individually between the RNC and the GSN entities, and between the GGSN and the P-CSCF.

In our opinion, the following reasons speak against such a solution:

- Protection of the IMS access network should be provided independent of the underlying technology. Therefore it does not seem to be a good approach to rely on the security of both the PS domain core network and the PS domain access network to secure IMS access network signaling.
- To secure SIP messages between UE and P-CSCF, it is not sufficient to secure e.g. all GTP-U traffic between SGSN and GGSN. In addition, it is still necessary to secure GTP-U traffic between RNC and SGSN (Iu-PS interface), as pointed out in [S3-010442], and signaling between GGSN and P-CSCF.
- We do not see any additional benefits from a security point of view, over the protection already provided by the IMS, that justifies the additional effort of any of the solutions 2 to 4 listed in [S3-010403]. In particular, SIP signalling messages are only a very small part of GTP-U traffic. It therefore seems not justified to apply encryption to all GTP-U traffic.
- In addition, there are concerns that encryption may cause delays which are not compatible with the requirements of real-time traffic.

Protecting IMS access domain messages by PS domain means could prevent attackers from successfully eavesdropping on the data between RNC and SGSN, or SGSN and GGSN. But as encryption is not even mandatory for the PS domain access network, this would only solve one part of the problem.

Conclusion and proposals

Altogether our clear impression is that there does not seem to be any obvious advantage of the required PS domain security extension, protecting IMS access domain signaling through GTP-U. We do not see a justification for the huge effort required for realising any of the options 2 to 4 listed in [S3-010403].

Therefore it is proposed to agree within SA3 on the working assumption that no PS core network domain security means are required for protecting IMS access network signaling (signaling between UE and P-CSCF).

Furthermore it is proposed to send an according liaison for clarification to SA2, CN1 and CN4.

References

[S3-010389] 3GPP TSG SA WG3 Security, S3-010389: "On the use of Network Domain Security for protection of SIP signaling messages". Source: Telenor, S3#19, 4 - 6 July 2001, London (UK).

[S3-010403] 3GPP TSG SA WG3 Security, S3-010403: "On the use of Network Domain Security for protection of SIP signaling messages". Source: SA3, S3#19, 4 - 6 July 2001, London (UK).

[S3-010433] 3GPP TSG SA WG3 Security, S3-010433: "LS S3-010403 on the use of Network Domain Security for protection of SIP signaling messages from WG3.". Source: SA2 meeting #19, 08/2001.

[S3-010442] 3GPP TSG SA WG3 Security, S3-010442: "Response to LS "On the use of Network Domain Security for protection of SIP signaling messages“ (N1-011041 or S3-010403)". Source: CN1 meeting #19, 08/2001.